

I claim:

1. A communication system comprising:
 - a rendezvous point device that forwards multicast communication messages to members of a shared tree;
 - a designated device in communication with the rendezvous point device via a number of intermediate devices; and
 - a host device in communication with the designated device, wherein:
 - the host device sends a join request to the designated device using a predetermined multicast group management protocol in order to join the shared tree for receiving the multicast communication messages forwarded by the rendezvous point device;
 - the designated device receives the join request and forwards to the rendezvous point device via the number of intermediate devices an encoded join request generated using an authentication key associated with the host device;
 - the rendezvous point device receives the encoded join request and authenticates the encoded join message using the authentication key associated with the host device; and
 - the host device is prevented from receiving the multicast communication messages forwarded by the rendezvous point device, if the rendezvous point device determines that the encoded join message is not authentic.
2. The communication system of claim 1, further comprising a key server for authenticating the host device and generating the authentication key for the host device.
3. The communication system of claim 2, wherein the key server provides the authentication key to both the host device and the rendezvous point device using a secure key distribution mechanism.
4. The communication system of claim 1, wherein the host device sends the authentication key to the designated device.

5. The communication system of claim 4, wherein the host device sends the authentication key to the designated device in the join request.
6. The communication system of claim 5, wherein the predetermined multicast group management protocol is an extended Internet Group Management Protocol (IGMP) including means for including the authentication key in the join request.
5
7. The communication system of claim 1, wherein the designated device joins the shared tree on behalf of the host device.
10
8. The communication system of claim 7, wherein the designated device establishes appropriate multicast routes for forwarding multicast communication messages to the host.
15
9. The communication system of claim 1, wherein each intermediate device receives the encoded join request and forwards the encoded join request toward the rendezvous point device.
20
10. The communication system of claim 9, wherein each intermediate device that is not already joined to the shared tree joins the shared tree on behalf of the host device and establishes appropriate multicast routes for forwarding multicast communication messages toward the host device upon receiving the encoded join request.
25
11. The communication system of claim 9, wherein each intermediate device that is already joined to the shared tree waits for an explicit acknowledgment message from the rendezvous point device and establishes appropriate multicast routes for forwarding multicast communication messages toward the host device only upon receiving the explicit acknowledgment message from the rendezvous point device.

12. The communication system of claim 1, wherein the rendezvous point device sends an explicit acknowledgment message toward the host device upon determining that the encoded join request is authentic.

13. A method comprising:
 - authenticating a host device;
 - generating an authentication key for the host device; and
 - sending the authentication key to the host device and to a rendezvous point device

5

using a secure key distribution mechanism.

14. An apparatus comprising:

authentication logic operably coupled to authenticate a host device;

key generation logic operably coupled to generate an authentication key for the host device; and

key distribution logic operably coupled to send the authentication key to the host device and to a rendezvous point device using a secure key distribution mechanism.

15. A computer readable medium having embodied therein a computer program for controlling a computer system, the computer program comprising:

authentication logic programmed to authenticate a host device;

key generation logic programmed to generate an authentication key for the host device; and

key distribution logic programmed to send the authentication key to the host device and to a rendezvous point device using a secure key distribution mechanism.

16. The computer readable medium of claim 15, wherein the computer readable medium is a computer storage medium.

17. The computer readable medium of claim 15, wherein the computer readable medium is a computer communication medium.

18. A method comprising:
 - obtaining an authentication key; and
 - sending a join request to a designated device using a predetermined multicast group management protocol, the join request including the authentication key.
 19. The method of claim 18, wherein the predetermined multicast group management protocol is an extended Internet Group Management Protocol (IGMP) including means for including the authentication key in the join request.

20. An apparatus comprising:
receiving logic operably coupled to receive an authentication key; and
joining logic operably coupled to send a join request to a designated device using a
predetermined multicast group management protocol, the join request including the
authentication key.
- 5
21. The apparatus of claim 20, wherein the predetermined multicast group
management protocol is an extended Internet Group Management Protocol (IGMP)
including means for including the authentication key in the join request.

22. A computer readable medium having embodied therein a computer program for controlling a computer system, the computer program comprising:

receiving logic programmed to receive an authentication key; and
group management logic programmed to send a join request to a designated device
using a predetermined multicast group management protocol, the join request including
the authentication key.

23. The computer readable medium of claim 22, wherein the predetermined multicast group management protocol is an extended Internet Group Management Protocol (IGMP) including means for including the authentication key in the join request.

24. The computer readable medium of claim 22, wherein the computer readable medium is a computer storage medium.

25. The computer readable medium of claim 22, wherein the computer readable medium is a computer communication medium.

26. A method comprising:
receiving a join request from a host device;
generating an encoded join request using an authentication key associated with the host device; and
5 sending the encoded join request toward a rendezvous point device.
27. The method of claim 26, wherein the join request includes the authentication key.
28. The method of claim 26, further comprising:
joining a shared tree on behalf of the host device and establishing appropriate multicast routes for forwarding multicast communication messages to the host device.

10

29. An apparatus comprising:

receiving logic operably coupled to receive a join request from a host device;

encoding logic operably coupled to generate an encoded join request using an authentication key associated with the host device; and

5 sending logic operably coupled to send the encoded join request toward a rendezvous point device.

30. The apparatus of claim 29, wherein the join request includes the authentication key.

10 31. The apparatus of claim 29, further comprising:

joining logic operably coupled to join a shared tree on behalf of the host device;

and

15 routing logic operably coupled to establish appropriate multicast routes for forwarding multicast communication messages to the host device.

CONTINUED ON BACK

32. A computer readable medium having embodied therein a computer program for controlling a computer system, the computer program comprising:

receiving logic programmed to receive a join request from a host device;
encoding logic programmed to generate an encoded join request using an authentication key associated with the host device; and
sending logic programmed to send the encoded join request toward a rendezvous point device.

5
10
33. The computer readable medium of claim 32, wherein the join request includes the authentication key.

15
34. The computer readable medium of claim 32, further comprising:
joining logic operably coupled to join a shared tree on behalf of the host device;
and
routing logic operably coupled to establish appropriate multicast routes for forwarding multicast communication messages to the host device.

20
35. The computer readable medium of claim 32, wherein the computer readable medium is a computer storage medium.

36. The computer readable medium of claim 32, wherein the computer readable medium is a computer communication medium.

37. A method comprising:
receiving an encoded join request for a host device; and
forwarding the encoded join request toward a rendezvous point device.
- 5 38. The method of claim 37, further comprising:
joining a shared tree for the host device; and
establishing appropriate multicast routes for forwarding multicast communication messages toward the host device.
- 10 39. The method of claim 37, further comprising:
waiting for an explicit acknowledgment message from the rendezvous point device; and
establishing appropriate multicast routes for forwarding multicast communication messages toward the host device only upon receiving the explicit acknowledgment message from the rendezvous point device.
- 15

40. An apparatus comprising:

receiving logic operably coupled to receive an encoded join request for a host device; and

forwarding logic operably coupled to forward the encoded join request toward a rendezvous point device.

5

41. The apparatus of claim 40, further comprising:

joining logic operably coupled to join a shared tree for the host device; and

routing logic operably coupled to establish appropriate multicast routes for forwarding multicast communication messages toward the host device.

10

42. The apparatus of claim 40, further comprising:

waiting logic operably coupled to wait for an explicit acknowledgment message from the rendezvous point device; and

routing logic operably coupled to establish appropriate multicast routes for forwarding multicast communication messages toward the host device only upon receiving the explicit acknowledgment message from the rendezvous point device.

15

43. A computer readable medium having embodied therein a computer program for controlling a computer system, the computer program comprising:

receiving logic programmed to receive an encoded join request for a host device; and

5 forwarding logic programmed to forward the encoded join request toward a rendezvous point device.

44. The computer readable medium of claim 43, further comprising:

joining logic programmed to join a shared tree for the host device; and

10 routing logic programmed to establish appropriate multicast routes for forwarding multicast communication messages toward the host device.

45. The computer readable medium of claim 43, further comprising:

15 waiting logic programmed to wait for an explicit acknowledgment message from the rendezvous point device; and

routing logic programmed to establish appropriate multicast routes for forwarding multicast communication messages toward the host device only upon receiving the explicit acknowledgment message from the rendezvous point device.

20 46. The computer readable medium of claim 43, wherein the computer readable medium is a computer storage medium.

47. The computer readable medium of claim 43, wherein the computer readable medium is a computer communication medium.

48. A method comprising:

receiving an encoded join request for a host device;

authenticating the encoded join request to determine whether or not the encoded join request is authentic; and

5 establishing appropriate multicast routes for forwarding multicast communication messages to the host device if and only if the encoded join request is determined to be authentic.

10 49. The method of claim 48, wherein authenticating the encoded join request comprises:

maintaining a number of authentication keys;

determining the host device for the encoded join request; and

searching for an authentication key associated with the host device.

15 50. The method of claim 49, wherein authenticating the encoded join request further comprises:

failing to find an authentication key associated with the host device; and

determining that the encoded join request is not authentic.

20 51. The method of claim 49, wherein authenticating the encoded join request further comprises:

finding an authentication key associated with the host device; and

authenticating the encoded join request using the authentication key associated with the host device.

25 52. The method of claim 48, further comprising:

sending an explicit acknowledgment toward the host device if and only if the encoded join request is determined to be authentic.

53. An apparatus comprising:

receiving logic operably coupled to receive an encoded join request for a host device;

authenticating logic operably coupled to authenticate the encoded join request to determine whether or not the encoded join request is authentic; and

routing logic operably coupled to establish appropriate multicast routes for forwarding multicast communication messages to the host device if and only if the encoded join request is determined to be authentic.

10 54. The apparatus of claim 53, wherein the authenticating logic is operably coupled to maintain a number of authentication keys, determine the host device for the encoded join request, and search for an authentication key associated with the host device.

15 55. The apparatus of claim 54, wherein the authenticating logic is operably coupled to determine that the encoded join request is not authentic if the authenticating logic fails to find an authentication key associated with the host device.

20 56. The apparatus of claim 54, wherein the authenticating logic is operably coupled to authenticate the encoded join request using an authentication key associated with the host device if the authenticating logic finds the authentication key associated with the host device.

57. The apparatus of claim 53, further comprising:

25 acknowledgment logic operably coupled to send an explicit acknowledgment toward the host device if and only if the encoded join request is determined to be authentic.

58. A computer readable medium having embodied therein a computer program for controlling a computer system, the computer program comprising:

receiving logic programmed to receive an encoded join request for a host device;

authenticating logic programmed to authenticate the encoded join request to

determine whether or not the encoded join request is authentic; and

routing logic programmed to establish appropriate multicast routes for forwarding multicast communication messages to the host device if and only if the encoded join request is determined to be authentic.

10 59. The computer readable medium of claim 58, wherein the authenticating logic is programmed to maintain a number of authentication keys, determine the host device for the encoded join request, and search for an authentication key associated with the host device.

15 60. The computer readable medium of claim 59, wherein the authenticating logic is programmed to determine that the encoded join request is not authentic if the authenticating logic fails to find an authentication key associated with the host device.

20 61. The computer readable medium of claim 59, wherein the authenticating logic is programmed to authenticate the encoded join request using an authentication key associated with the host device if the authenticating logic finds the authentication key associated with the host device.

25 62. The computer readable medium of claim 58, further comprising:

acknowledgment logic programmed to send an explicit acknowledgment toward the host device if and only if the encoded join request is determined to be authentic.

63. The computer readable medium of claim 58, wherein the computer readable medium is a computer storage medium.

64. The computer readable medium of claim 58, wherein the computer readable medium is a computer communication medium.

65. In a communication system having a host device, a designated device, and a rendezvous point device, a method comprising:

sending a join request by the host device to the designated device in order to join a shared tree;

5 sending an encoded join request by the designated device to the rendezvous point device;

authenticating the encoded join request by the rendezvous point device;

adding the host device to the shared tree, if the encoded join request is authentic;
and

10 excluding the host device from the shared tree, if the encoded join request is not authentic.

66. A communication message embodied in a data signal, the communication message comprising a group key for a multicast group and an authentication key for a host device.

5 67. A communication message embodied in a data signal, the communication message comprising a join request including an authentication key for a host device.

68. A communication message embodied in a data signal, the communication message comprising an encoded join request including a tag field and a nonce field.

10 69. A communication message embodied in a data signal, the communication message comprising an explicit acknowledgment including a tag field and a nonce field.